Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

13 November 2017

PIN Number

171113-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released TLP:AMBER: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Individuals Initiate Fraudulent Payment Transactions using Unauthorized Financial Institution Routing Numbers

This notification was created jointly by the FBI and the National Cyber Forensics & Training Alliance (NCFTA).

Summary

Online actors are promoting a scam falsely claiming US citizens can access funds housed at Federal Reserve Banks free of charge. The online actors often advertise the scam as a way to pay personal online bills. They instruct victims to send payments from Federal Reserve Bank accounts to other bank accounts and institutions that accept Automated Clearing House (ACH) transfers. Some financial institutions have reported thousands of attempted transactions from non-existent Federal Reserve Bank, US Treasury, or other financial institutions' accounts since mid-2017. The attempted payments using the Federal Reserve Bank routing numbers are being rejected and returned unpaid. However, financial institutions may experience a loss if they credit an individual's account before the account holding institution rejects the requested funds.

Threat

Individuals conducting this scam:

- Fraudulently use Federal Reserve Bank routing numbers and fictitious account information to initiate debits from the fictitious accounts.
- May attempt to send payments using direct debits via e-commerce sites, third party payment applications, or account-to-account transfers, such as ACH items and e-checks.
- Have used the routing numbers for fraudulent check deposits and withdrawal of funds via ATM before the check is returned.
- Have used routing numbers not associated with Federal Reserve Banks. Some of the additional routing numbers were associated with the US Treasury, according to online posts in July 2017.

According to statements from the Federal Reserve Banks, consumers cannot use Federal Reserve Banks' routing numbers to make debit payments. Federal Reserve Banks provide banking services to banks and governmental entities, not to individuals. Attempts by individuals to initiate debit transactions using Federal Reserve Banks' routing numbers will be rejected and returned unpaid by Federal Reserve Banks.

Recommendations:

The FBI and the NCFTA recommend information security, fraud, or investigative groups processing or reviewing debit transactions, including checks, ACH debit items, e-check, and direct debit bill pay consider:

- Reviewing internal procedures for validating debit transactions before processing them or making funds available.
- Establishing ways to mitigate fraudulent payments involving the Federal Reserve Banks and other unauthorized routing numbers.

As with any routing number, Federal Reserve Banks' routing numbers are used for legitimate payment activity, which may include:

- Credit transfers (either wire or ACH credits) to and from a Federal Reserve Bank and another party.
- ACH debit transfers initiated by Federal Reserve Banks or by certain businesses or financial institutions.
- Checks sent by a Federal Reserve Bank to another financial institution, and, in limited circumstances, checks drawn on a Federal Reserve Bank to pay valid Federal Reserve Bank obligations.

In developing an approach to deal with the scheme, consider applying heightened scrutiny to debit transactions initiated by individuals seeking to obtain payment using the following Federal Reserve Bank routing numbers. (The below list of routing numbers should not be considered an exhaustive list. Additional routing numbers are likely associated with the scheme.)

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

(U) Unauthorized Routing Numbers

b7E

Administrative Note

This product is marked TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey